



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/799,455

03/12/2004

Sean E. Purcell

308121.01/MFCP.149221

7697

45809

7590

03/12/2010

SHOOK, HARDY & BACON L.L.P.
(MICROSOFT CORPORATION)
INTELLECTUAL PROPERTY DEPARTMENT
2555 GRAND BOULEVARD
KANSAS CITY, MO 64108-2613

EXAMINER

MAI, KEVIN S

ART UNIT

PAPER NUMBER

2456

MAIL DATE

DELIVERY MODE

03/12/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/799,455	Applicant(s) PURCELL ET AL.	
	Examiner KEVIN S. MAI	Art Unit 2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 December 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7,9-13,15-20,22,24,25,27,29,30 and 34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7,9-13,15-20,22,24,25,27,29,30 and 34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>12/3/09</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action has been issued in response to Applicant's Amendment filed December 18, 2009.

2. Claims 1-7, 9-13, 15-20, 22, 24, 25, 27, 29, 30 and 34 have been amended. Claims 1-7, 9-13, 15-20, 22, 24, 25, 27, 29, 30 and 34 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed December 18, 2009 have been fully considered but they are not persuasive.

4. Applicant's arguments with respect to Daniell's obviousness rejection of claim 1 have been considered but they are not persuasive. Applicant argues that the claimed system filters and blocks a great deal more than a parent would be capable of. Applicant points to Andrews to discuss that neither the byte patterns nor the e-mail header could be filtered by the parent. Applicant further argues that the throughput of Applicant's invention is well beyond the capabilities of any parent. Applicant also argues that the system requires a processor. Examiner disagrees.

5. Examiner would like to point out that arguments geared toward filtering byte patterns and the e-mail header are arguing points that are not claimed in the limitations. The claim only discusses identifying offensive portions of messages and similarly only blocking offensive portions. There is no discussion of byte patterns or e-mail headers being filtered. As such arguments towards a person's inability to perform such features are currently moot.

Art Unit: 2456

6. Examiner further argues that there is no need for the parent to perform the filtering portion. Daniell already discloses filtering to identify, as seen in figure 9B the system discloses to the parent the objectionable words/phrases that have been detected. As such arguments toward whether or not a person could perform the filtering portions are seen to be moot.

7. Examiner further argues that the throughput of the invention does not alter the argument made previously in view of *In re Venner*, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). The court held that broadly providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. The automation of blocking offensive portions is seen to simply be automation of the manual activity of selecting to block filtered words as seen in figure 9B of Daniell. In addition, with respect to applicant's arguments requiring a processor it is seen that such a feature is obvious in view of this being implemented in Daniell which includes a processor.

8. Accordingly, examiner maintains that these features are obvious in view of *In re Venner*, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958).

9. Applicant's arguments with respect to Daniell and Chupin's rejection of claims 1, 5, 6 and 10 have been considered but they are not persuasive. Applicant argues that the entire Chupin document just describes restricting e-mail content to an approved list of senders and screening content. Chupin is silent as to displaying non-offensive portions of the message. Examiner disagrees. Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email. It is seen that if the

Art Unit: 2456

offensive words are filtered from the email then non offensive words would remain in the email. Accordingly the non-offensive words would be displayed.

10. Applicant further argues the claim has been amended to also require “a content blocking computer-executable component, triggered when a junk score of the message exceeds a first threshold level, which block the offensive portions ...” and that neither Daniell nor Chupin disclose this. However, as mentioned previously in similar limitations, Rajan discloses this. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

11. Applicant’s arguments with respect Daniell, Chupin and Rajan’s rejection to claims 2-4, 7, 9, 18-20, 22, 24, 25, 27 and 34 have been considered but they are not persuasive. Applicant

Art Unit: 2456

argues Rajan is directed to classification of email and does not compensate for the deficiencies of Daniell and Chupin. Examiner disagrees. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

12. Applicant further argues that the entire Chupin document just describes restricting e-mail content to an approved list of senders and screening content. Chupin is silent as to displaying non-offensive portions of the message. Examiner disagrees. Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email. It is seen that if the offensive words are filtered from the email then non offensive words would remain in the email. Accordingly the non-offensive words would be displayed.

Art Unit: 2456

13. Applicant further argues that claims 22 and 34 have been amended to also required "enabling a user to preview the non-offensive portions ... while blocking the offensive portions ... when the junk score exceeds a first threshold level; and issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level, wherein the first threshold level differs from the second threshold level". However, as mentioned previously in similar limitations, Rajan and Andrews discloses these features. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score and furthermore to perform different actions according to various thresholds. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

14. Then as to the challenge Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears

Art Unit: 2456

to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Chupin-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

15. Applicant's arguments with respect Daniell and Rajan's rejection to claims 22 and 34 have been considered but they are not persuasive. Applicant argues that claims 22 and 34 have been amended to also required "enabling a user to preview the non-offensive portions ... while blocking the offensive portions ... when the junk score exceeds a first threshold level; and issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level, wherein the first threshold level differs from the second threshold level". However, as mentioned previously in similar limitations, Rajan and Andrews discloses these features. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail

Art Unit: 2456

is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score and furthermore to perform different actions according to various thresholds. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

16. Then as to the challenge Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Chupin-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine.

Art Unit: 2456

Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

17. Applicant argues Rajan is directed to classification of email and does not compensate for the deficiencies of Daniell. Examiner disagrees. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

18. Applicant's argument's with respect to claim 11 are the same as those used for claim 1 and as such examiner provides the same rationale used above.

19. Applicant's arguments with respect Daniell, Chupin, Rajan and Andrew's rejection to claims 12, 13, 15-17 and 30 have been considered but they are not persuasive. Applicant argues

Art Unit: 2456

Rajan is directed to classification of email and does not compensate for the deficiencies of Daniell and Chupin. Examiner disagrees. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

20. Applicant further argues that the claims require the challenge be triggered when the junk score of the message exceeds a second threshold. However, as mentioned previously in similar limitations, Rajan and Andrews discloses these features. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears

Art Unit: 2456

with the regular mail according to its level of spaminess. As such it is well known to perform actions on emails according to a junk score and furthermore to perform different actions according to various thresholds. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan).

21. Then as to the challenge Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Chupin-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

Art Unit: 2456

22. Applicant's argument's with respect to claim 29 are the same as those used for claim 22 and as such examiner provides the same rationale used above.

Claim Rejections - 35 USC § 103

23. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

24. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pub. No. 2005/0097174 to Daniell et al. (hereinafter "Daniell") and further in view of U.S. Pub. No. 2005/0165895 to Rajan et al. (hereinafter "Rajan").

25. As to Claim 1, Daniell discloses a **computer-implemented system using processor, memory, and data storage subsystems** that mitigates viewing offensive message content, **the computer-implemented system** comprising:
a processor that executes the following computer executable components stored on a computer readable medium (Figure 1 and paragraph [0024] of Daniell disclose a processor);
a message receiving computer-executable component that receives a message for delivery to a user input device (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);
a filtering computer-executable component that that identifies offensive portions of the message, the message comprising one or more of text, images, sounds, videos, URLs,

Art Unit: 2456

embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases); **and a content blocking computer-executable component, [triggered when a junk score of the message exceeds a first threshold level], which blocks the offensive portions of the message by preventing the offensive portions thereof from being viewed or sensed from at least a preview pane that displays the message, [and fully displays non-offensive portions of the message]** (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired).

Daniell does not explicitly disclose **triggered when a junk score of the message exceeds a first threshold level**

However, Rajan discloses this. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Daniell-Chupin, with calculating a junk score as disclosed by Rajan. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding

Art Unit: 2456

algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan)

Daniell does not explicitly disclose **and fully displays non-offensive portions of the message.**

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This is seen to be disclosing partially blocking content by preventing offensive portions of the message from being viewed and also displaying non-offensive portions of the message. While this is being done manually by a parent for a child it nonetheless discloses the email client containing a feature used to detect objectionable words for the purpose of replacing them with acceptable words to prevent only the objectionable content from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine preventing messages from being viewed in the preview pane as disclosed by Daniell, with preventing only the objectionable content from being viewed as disclosed by Daniell. One of ordinary skill in the art would have been motivated to combine to prevent unintentional viewing of content determined to be objectionable or undesired. Since the purpose of a spam filtering is to prevent the user from viewing content they do not wish to view, it would be obvious to prevent the user from seeing the content via the preview pane because the content has been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

Art Unit: 2456

26. Claims 1-7, 9, 10 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell and further in view of Rajan and further in view of US Pat. No. 7222309 to Chupin et al. (hereinafter “Chupin”).

27. As to Claim 1, Daniell discloses a computer-implemented system using processor, memory, and data storage subsystems that mitigates viewing offensive message content, the computer-implemented system comprising:

a processor that executes the following computer executable components stored on a computer readable medium (Figure 1 and paragraph [0024] of Daniell disclose a processor); a message receiving computer-executable component that receives a message for delivery to a user (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

a filtering computer-executable component that that identifies offensive portions of the message, the message comprising one or more of text, images, sounds, videos, URLs, embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases); and a content blocking computer-executable component, [triggered when a junk score of the message exceeds a first threshold level, which] blocks the offensive portions of the message by preventing the offensive portions thereof from being viewed or sensed from at least a preview pane that displays the message, [and fully displays non-offensive portions of the message] (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of

Art Unit: 2456

displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired).

Daniell does not explicitly disclose **triggered when a junk score of the message exceeds a first threshold level**

However, Rajan discloses this. Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages. Paragraph [0015] further discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the system of claim 1 as disclosed by Daniell, with calculating a junk score as disclosed by Rajan. One of ordinary skill in the art would have been motivated to combine because both systems disclose spam filtering and as such substituting one systems spam finding algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as simple substitution of one known element for another. Wherein one of ordinary skill in the art would be further motivated to combine to improve the situation where too many or too few emails are classified as spam (Paragraphs [0009] and [0010] of Rajan)

Daniell does not explicitly disclose **and fully displays non-offensive portions of the message.**

Art Unit: 2456

However, Chupin discloses this (Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine disabling a preview pane as disclosed by Daniell, with filtering out offensive words as disclosed by Chupin. One of ordinary skill in the art would have been motivated to combine to use a known technique to improve similar devices in the same way. Since both inventions are geared toward preventing users from viewing offensive content it would be obvious to implement the features of one into the other.

28. As to Claim 2, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 1, further comprising**

a classification computer-executable component that classifies the message as any one of a good state, a junk state, and a middle state based in part on the junk score (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. This is seen to be the same as having a good, junk, and middle state.)

wherein the middle state indicates that the message is determined to be safe for an inbox, but not safe for viewing or previewing in at least the preview pane without blocking the offensive portions of the message (Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory such as the inbox (white) directory and the gray directory.

Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a

Art Unit: 2456

selected message can be disabled for spam messages. Thus it is seen that those that are rated gray/white would be in the inbox but since it is spam would still have the have the content be filtered as disclosed in Daniell-Chupin).

Examiner recites the same rationale to combine used in claim 1.

29. **As to Claim 3**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 2, wherein the message is classified at least in the middle state when the junk score exceeds at least the first threshold** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Thus it is seen that exceeding the first threshold of 30 in this situation would be classifying a message in the middle state).

Examiner recites the same rationale to combine used in claim 1.

30. **As to Claim 4**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 2, further comprising an analysis computer-executable component that determines whether the junk score exceeds a first threshold** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. This classification step is seen to imply that determination of a message exceeding a threshold is done by the system).

Examiner recites the same rationale to combine used in claim 1.

31. **As to Claim 5**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 1, further comprising an unblocking computer-executable component that receives user input to unblock the offensive portions of the message in at least the preview pane** (Paragraph [0044] of Daniell discloses that messages in the spam folder may be unmarked as spam and the message that has been stored in the spam folder would be moved to the inbox folder of the user. Since the preview pane is fully enabled in the inbox it is seen that the blocked portion of the message would now be unblocked and viewable in the preview pane).

32. **As to Claim 6**, Daniell-Rajan-Chupin discloses **wherein the computer-implemented system of claim 5, the unblocking computer-executable component operates per message** (Paragraph [0044] of Daniell discloses that messages in the spam folder may be unmarked as spam and the message that has been stored in the spam folder would be moved to the inbox folder of the use. This only being applied to the selected message and as such is operating per message).

33. **As to Claim 7**, Daniell-Rajan-Chupin discloses **wherein the computer-implemented e system of claim 1 the content blocking computer-executable component operates per message or globally for substantially all messages** (Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory such as the inbox (white) directory and the gray directory. Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a selected message can be disabled for spam messages. Thus it is seen that those

Art Unit: 2456

that are rated gray/white would be in the inbox but since it is spam those messages would still have the preview disabled. This scenario represents blocking operating per message. However in paragraph [0043] of Daniell the preview window being disabled applies to the whole spam folder, this implies the ability to disable the preview window for specific folders. If all folders were then disabled it would be the same as the blocking component operating globally.)

Examiner recites the same rationale to combine used in claim 1.

34. As to Claim 9, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 4, the first threshold level determined in part by user preferences** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. These ranges are seen to be the same as the thresholds).

Examiner recites the same rationale to combine used in claim 1.

35. As to Claim 10, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 1. Daniell-Chupin does not explicitly disclose wherein the content blocking computer-executable component blocks the offensive portions of the message by utilizing at least one of the following:**

a blocked portion of a subject line of the message;

a blocked portion of a from line of the message;

a blurred portion of the subject line of the message;

a blurred portion of the from line of the message; or

Art Unit: 2456

a blurred portion of the message in at least the preview pane.

However, such a feature is implied by Chupin. Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email. Since offensive words are filtered from the email, it is seen that any such instances of these words would be filtered including those in the subject line of the message. Such an implementation would be obvious to try in view of Chupin's disclosure.

36. **As to Claim 18**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 1, further comprising a rating computer-executable component that rates messages as unscanned before the messages are subjected to the filtering computer-executable component** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

Examiner recites the same rationale to combine used in claim 1.

37. **As to Claim 19**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 18, wherein an unscanned message is hidden from view and is not visible in the user's inbox while additional data about the unscanned message is collected or while the unscanned message is being filtered by the filtering computer-executable component** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is

Art Unit: 2456

graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded. Since they are not placed into the inbox until after filtering, the messages are effectively hidden from view and are not visible).

Examiner recites the same rationale to combine used in claim 1.

38. **As to Claim 20**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 18, wherein unscanned messages are made visible in a user's inbox when the filtering component is turned off** (Figure 4 of Daniell discloses being able to turn off spam filtering and next to the selection it is explained that all emails will be delivered to the inbox. Thus it is seen that when filtering is off all messages would be visible).

It is seen that being able to turn off the filter is an obvious feature of the system. Furthermore, once the filter is turned off it is disclosed in Daniell that all emails will be delivered to the inbox. Given that nothing will be marked as spam, none of them would be blocked and as such they would all be visible. Thus it is seen that this limitation is disclosed by Daniell.

39. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-Rajan-Chupin and further in view of U.S. Pub. No. 2003/0009495 to Adjaoute (hereinafter "Adjaoute").

40. **As to Claim 11**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 1**. Daniell-Rajan-Chupin does not explicitly disclose **wherein the content blocking**

Art Unit: 2456

computer-executable component replaces blocked offensive portions of the message with at least one of a text notice, a graphics notice, a video notice, or an audio notice; and wherein the text notice, the graphics notice, the video notice and the audio notice warn users that potentially offensive content has been blocked from view.

However, Adjaoute discloses this (Paragraph [0057] of Adjaoute discloses that if the content is restricted, then a message is displayed instead of the content saying that the access to the content has been restricted. It is noted that Adjaoute deals primarily with websites however in paragraph [0029] it suggest the software plug-in being installed in an email application).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Rajan-Chupin, with replacing the blocked content as disclosed by Adjaoute. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to help the filter prevent viewing of offensive material. Paragraph [0006] of Adjaoute shares that the goal would be to control the information that children can receive. Thus it is seen that it would be advantageous to block the material and inform the participant that what they are trying to access has been blocked.

41. Claims 22 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell and further in view of Rajan and further in view of U.S. Pub. No. 2003/0204569 to Andrews et al. (hereinafter "Andrews").

Art Unit: 2456

42. As to Claim 22, Daniell discloses a **computer-implemented method using processor, memory, and data storage subsystems** that mitigates viewing offensive message content comprising:

executing computer executable instructions stored on a computer readable medium of **the processor, the computer executable instructions comprising** (Figure 1 and paragraph [0024] of Daniell disclose a processor);

receiving a message into the memory of the processor (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

[computing a junk score for the message];

determining offensive portions and non-offensive portions of the message, wherein the message comprises one or more of text, images, sounds, videos, URLs, embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases); **and**

enabling a user to preview the [non-offensive portions of the] message in at least a preview pane while blocking the offensive portions of the message from the user [when the junk score exceeds a first threshold level] (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired)

[issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level, wherein]

[the first threshold level differs from the second threshold level]

Art Unit: 2456

Daniell does not explicitly disclose **computing a junk score for the message**.

However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combined used in claim 1.

Daniell does not explicitly disclose enabling a user to preview the **non-offensive portions of the** message.

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This is seen to be disclosing partially blocking content by preventing offensive portions of the message from being viewed and also displaying non-offensive portions of the message. While this is being done manually by a parent for a child it nonetheless discloses the email client containing a feature used to detect objectionable words for the purpose of replacing them with acceptable words to prevent only the objectionable content from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine preventing messages from being viewed in the preview pane as disclosed by Daniell, with preventing only the objectionable content from being viewed as disclosed by Daniell. One of ordinary skill in the art would have been motivated to combine to prevent unintentional viewing of content determined to be objectionable or undesired. Since the purpose of a spam filtering is to prevent the user from viewing content they do not wish to view, it would be

Art Unit: 2456

obvious to prevent the user from seeing the content via the preview pane because the content has been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

Daniell does not explicitly disclose altering the ability to preview **when the junk score exceeds a first threshold level**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Chupin-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is

Art Unit: 2456

generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

Daniell does not explicitly disclose **the first threshold level differs from the second threshold level**

However, Rajan discloses this. Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Accordingly it is well known to perform different action according to various thresholds.

Examiner recites the same rationale to combine used in claim 1.

43. As to Claim 34, Daniell discloses a **computer-implemented system using processor, memory, and data storage subsystems to mitigate viewing offensive message content**

comprising:

means for receiving a message (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

[means for computing a junk score for the message];

means for determining offensive portions and non-offensive portions of the message, the message comprising one or more of text, images, sounds, videos, URLs, embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases); **and**

Art Unit: 2456

means for blocking the offensive portions of the message associated with information deemed offensive to the user from being presented to the user, [and displaying the non-offensive portions] when the message is displayed in at least a preview pane, [when the junk score exceeds a first threshold level] (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess) **[means for issuing a challenge message to the sender of the message when the junk score exceeds a second threshold level];**

wherein instructions associated with one or more of the above means are executed by the processor operatively coupled to the memory of the computer-implemented system (Figure 1 and paragraph [0024] of Daniell disclose a processor coupled to memory).

Daniell does not explicitly disclose **means for computing a junk score for the message.**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **and displaying the non-offensive portions.**

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This is seen to be disclosing partially blocking content by preventing offensive portions of the message from being viewed and also displaying non-offensive portions of the message. While

Art Unit: 2456

this is being done manually by a parent for a child it nonetheless discloses the email client containing a feature used to detect objectionable words for the purpose of replacing them with acceptable words to prevent only the objectionable content from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to combine preventing messages from being viewed in the preview pane as disclosed by Daniell, with preventing only the objectionable content from being viewed as disclosed by Daniell. One of ordinary skill in the art would have been motivated to combine to prevent unintentional viewing of content determined to be objectionable or undesired. Since the purpose of a spam filtering is to prevent the user from viewing content they do not wish to view, it would be obvious to prevent the user from seeing the content via the preview pane because the content has been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

Daniell does not explicitly disclose altering the ability to preview **when the junk score exceeds a first threshold level**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **means for issuing a challenge message to the sender of the message**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a

Art Unit: 2456

message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 22.

Daniell does not explicitly disclose **when the junk score exceeds a second threshold level**

However, Rajan discloses this. Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Accordingly it is well known to perform different action according to various thresholds.

Examiner recites the same rationale to combine used in claim 1.

44. Claims 12, 13, 15-17, 22, 24, 25, 27, 30 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-Chupin-Rajan and further in view of Andrews.

45. **As to Claim 12**, Daniell-Rajan-Chupin discloses **the computer-implemented system of claim 2**. Daniell-Rajan-Chupin does not explicitly disclose **further comprising a challenge-response computer-executable component comprising:**
a challenge activation computer-executable component, triggered when the junk score of the message exceeds a second threshold level;
a challenge message sent to a sender of the message;

Art Unit: 2456

**a challenge puzzle or question completed by the sender of the message; and
a response receiving computer-executable component for validation of the sender's
response to the challenge puzzle or question and transfer of the message to the user's inbox
upon validation**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 22.

46. **As to Claim 13**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented system of claim 12, wherein the second threshold level is higher or lower than the first threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. It is noted that because Rajan discloses a user setting up the configurations for his various spam directories that it would be obvious to either have the second threshold higher or lower depending on the personal preference of the user).

Examiner recites the same rationale to combine used in claim 1.

Art Unit: 2456

47. **As to Claim 15**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented system of claim 12, wherein the second threshold level is determined at least in part by user preferences** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. These ranges are seen to be the same as the thresholds).

Examiner recites the same rationale to combine used in claim 1.

48. **As to Claim 16**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented system of claim 12, wherein the message sent by the respective message sender is hidden from view in a user's inbox until the at least one challenge is correctly solved** (Figure 1 of Andrews discloses a letter being detained in the smart email filtering system until a correct response is received. This is effectively hiding the message from view until it is correctly solved).

Examiner recites the same rationale to combine used in claim 22.

49. **As to Claim 17**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented system of claim 12, wherein offensive portions of the message sent by the respective message sender are blocked when the message is released to the user's inbox following a correctly solved challenge** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message is issued a challenge. Then in paragraph [0087] of

Art Unit: 2456

Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. It is seen that since the letter was placed into the inbox and that, as disclosed above, letters in the inbox with sufficient ratings are blocked, it would be obvious that after a message comes back from a challenge that it would still be blocked once deposited in the inbox).

Examiner recites the same rationale to combine used in claim 22.

50. As to Claim 22, Daniell discloses a **computer-implemented method using processor, memory, and data storage subsystems** that mitigates viewing offensive message content comprising:

executing computer executable instructions stored on a computer readable medium of the processor, the computer executable instructions comprising (Figure 1 and paragraph [0024] of Daniell disclose a processor);

receiving a message into the memory of the processor (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

[computing a junk score for the message];

determining offensive portions and non-offensive portions of the message, wherein the message comprises one or more of text, images, sounds, videos, URLs, embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases);

Art Unit: 2456

enabling a user to preview the [non-offensive portions of the] message in at least a preview pane while blocking the offensive portions of the message from the user [when the junk score exceeds a first threshold level] (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired); and [issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level], wherein [the first threshold level differs from the second threshold level]

Daniell does not explicitly disclose **computing a junk score for the message.**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose enabling a user to preview the **non-offensive portions of the** message.

However, Chupin discloses this (Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email)

Examiner recites the same rationale to combine used in Claim 1.

Daniell does not explicitly disclose altering the ability to preview **when the junk score exceeds a first threshold level**

Art Unit: 2456

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **issuing a challenge message to the sender of the message, triggered when the junk score exceeds a second threshold level**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Chupin-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

Daniell does not explicitly disclose **the first threshold level differs from the second threshold level**

Art Unit: 2456

However, Rajan discloses this. Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Accordingly it is well known to perform different action according to various thresholds.

Examiner recites the same rationale to combine used in claim 1.

51. **As to Claim 24**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented method of claim 22, further comprising classifying the message as unscanned before computing the junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

Examiner recites the same rationale to combine used in claim 1.

52. **As to Claim 25**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented method of claim 24, further comprising updating the message from unscanned to some other rating based on, at least in part, its computed junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating

Art Unit: 2456

and are only moved to the inbox after being graded. However after being graded it is then moved to the appropriate directories at which point it would be classified under those directories. Thus the score is seen to be updated).

Examiner recites the same rationale to combine used in claim 1.

53. As to **Claim 27**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented method of claim 22, further comprising unblocking the blocked offensive portions of the message when explicit user input to unblock the blocked message offensive portions is received** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This allows the user to read the text associated with the selected message. Since the message that was in the spam folder was previously not viewable in the preview screen (blocked) and then distinct user input (selecting the read button) allows the letter to be read (unblocked), this is seen to be the same as the claimed limitation).

54. As to **Claim 30**, Daniell-Rajan-Chupin-Andrews discloses **the computer-implemented method of claim 22 further comprising challenging a sender of the message before revealing any blocked offensive portions of the message, wherein challenges are sent to the sender at a rate determined by a frequency or number of messages sent to the user** (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things, the message

Art Unit: 2456

is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox. Paragraph [0056] further discloses utilizing historical sender information in the decision in whether or not to issue a challenge. Accordingly it would have been obvious to utilize the number/frequency of messages sent to the user as criteria of the historical sender information as it is a well known criteria used in spam detection).

Examiner recites the same rationale to combine used in claim 22.

55. As to Claim 34, Daniell discloses a computer-implemented system using processor, memory, and data storage subsystems to migrate viewing offensive message content comprising:

means for receiving a message (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

[means for computing a junk score for the message];

means for determining offensive portions and non-offensive portions of the message, the message comprising one or more of text, images, sounds, videos, URLs, embedded content, attachments, or applets (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases); **and**

means for blocking the offensive portions of the message associated with information deemed offensive to the user from being presented to the user, [and displaying the non-offensive portions] when the message is displayed in at least a preview pane, [when the

Art Unit: 2456

junk score exceeds a first threshold level] (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess) **[means for issuing a challenge message to the sender of the message when the junk score exceeds a second threshold level];**

wherein instructions associated with one or more of the above means are executed by the processor operatively coupled to the memory of the computer-implemented system (Figure 1 and paragraph [0024] of Daniell disclose a processor coupled to memory).

Daniell does not explicitly disclose **means for computing a junk score for the message.**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **and displaying the non-offensive portions.**

However, Chupin discloses this (Column 7 lines 30-35 of Chupin disclose content screening of incoming email can be applied so that offensive words are filtered from the email);

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose altering the ability to preview **based on the junk score**

Art Unit: 2456

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose **means for issuing a challenge message to the sender of the message**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 22.

Daniell does not explicitly disclose **when the junk score exceeds a second threshold level**

However, Rajan discloses this. Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. Accordingly it is well known to perform different action according to various thresholds.

Examiner recites the same rationale to combine used in claim 1.

Art Unit: 2456

56. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-Rajan-Chupin-Andrews and further in view of U.S. Pub. No. 2005/0080889 to Malik et al. (hereinafter "Malik").

57. **As to Claim 29**, Daniell-Rajan-Chupin-Andrews disclose **the computer-implemented method of claim 22**. Daniell-Rajan-Chupin-Andrews does not explicitly disclose **further comprising requiring entry of a password to open messages associated with blocked offensive portions**.

However, Malik discloses this (Paragraph [0071] of Malik discloses child protection in an email system where it can be set such that to get access to a child's spam folder one would have to enter in the master or parent password. This is seen to be the same as needing a password to access messages that are blocked).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of claim 22 as disclosed by Daniell-Rajan-Chupin-Andrews, with requiring a password as disclosed by Malik.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to prevent children from viewing content that a parent would deem inappropriate for viewing. Thus it is to provide a method that restricts a child type user from performing a restricted operation (paragraph [0007] Malik).

Conclusion

58. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2456

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. S. M./
Examiner, Art Unit 2456

/Rupal D. Dharia/
Supervisory Patent Examiner, Art Unit 2400